
Project QC-2026-01

Standard *CIP-015-01* – *Cyber security – Internal Network Security Monitoring (INSM)*

1.1. Applicability

The following table lists the functional entities to which CIP-015-1, the reliability standard proposed for adoption (the “Reliability Standard”), applies.

Standard	Functions
CIP-015-1	<i>Balancing Authority (BA)</i> <i>Distribution Provider (DP)</i> <i>Generator Operator (GOP)</i> <i>Generator Owner (GO)</i> <i>Reliability Coordinator (RC)</i> <i>Transmission Operator (TOP)</i> <i>Transmission Owner (TO)</i>

1.2. Purpose of the standard

This section describes the purpose of the standard that is the subject of this request. The title and purpose of the standard are as follows:

- **CIP-015-1 – Cyber Security – Internal Network Security Monitoring:** To improve the probability of detecting anomalous or unauthorized network activity in order to facilitate improved response and recovery from an attack.

1.3. Regulatory context

Following the FERC Order 887¹, Docket n° RM22-3-000 issued on January 19, 2023, NERC received the order to develop a reliability standard concerning internal security monitoring of high-impact *BES* electronic systems with or without routable external connectivity, as well as for medium-impact *BES* systems with routable external connectivity. Therefor, NERC had to address this reliability gap to improve detecting capabilities of lateral movements by malicious actors.

The reliability standard CIP-015-1 was adopted by the NERC Board of Trustees on May 9th, 2024. NERC then filed a request with the FERC on June 24th, 2024, seeking approval for the new standard under Section 215² of the Federal Power Act. It was subsequently approved by the FERC on June 26th, 2025, as part of Order 907³, confirming its inclusion in the U.S. reliability standards.

¹ FERC Order 887, retrieved on March 17th, 2026: https://elibrary.ferc.gov/eLibrary/filelist?accession_number=20230119-3085&optimized=false.

² FERC Federal Power Act, Section 215 (p.67/102), retrieved on March 17th, 2026: https://www.ferc.gov/sites/default/files/2021-04/federal_power_act.pdf.

³ FERC Order 907, retrieved on March 17th, 2026: https://elibrary.ferc.gov/eLibrary/filelist?accession_num=20250626-3039.

The CIP-015-1⁴ standard, developed within the framework of NERC Project 2023-03⁵, is part of the evolution of the North American regulatory framework, aiming to protect the main transmission network (*BES*). Consequently, the objective of CIP-015-1 is to impose the implementation of mechanisms to ensure continuous monitoring of internal flows, the detection and assessment of abnormal activities, and the preservation and protection of necessary monitoring data to support appropriate responses to cybersecurity incidents. Thus, the implementation of Project 2023-03 marks a significant change by assisting existing perimeter controls with enhanced capabilities for detection and analysis within critical environments operated by transmission operators, generators, reliability coordinators, and other *BES*-responsible entities.

The Quebec Reliability Coordinator (hereinafter, the "Reliability Coordinator") submits in this filing the first regulatory filing of the *regulatory standard* CIP-015-1 of Project 2023-03 with the Régie de l'Énergie (hereinafter, the "Régie"). FERC Order 907 also discussed a second version of the standard CIP-015, aiming to extend the regulation to not only internal network monitoring obligation but also to *Electronic Access Control Monitoring Systems (EACMS)* and *Physical Access Control Systems (PACS)* located outside the electronic security perimeter, while specifying that only communication flows between CIP assets are targeted, will be addressed in a future regulatory filing.

1.4. Specific provisions for Québec

The Reliability Coordinator proposes this first Quebec-specific provision regarding the applicability of the standard:

"This standard applies only to facilities of the *Main Transmission System (RTP)* and to designated Distribution Provider facilities. When applying this standard, any reference to the terms *Bulk Electric System* or *BES* shall be replaced by the terms *Main Transmission System* or *RTP*, respectively."

The Reliability Coordinator is of the opinion that this special provision is applicable since the scope of application equivalent to the *BES* for Québec and recognized by the Régie is the *RTP*.

Secondly, the Reliability Coordinator proposes the following additional exemptions:

"The following are exempt from this standard:

- Any generation facility that meets both of the following conditions: (1) the rated power of the facility is 300 MVA or less and (2) none of the generating units of the facility can be synchronized with a *neighboring System*.
- Step-up substations of generating facilities that meet the conditions mentioned above."

The Reliability Coordinator agrees that the special provision with respect to the additional exemptions is applicable because of the exemption criteria mentioned above only references to low-impact facilities.

⁴ *Reliability Standard* CIP-015-1 from the NERC, retrieved on March 17th, 2026: [2023-03-cip-015-1-fb-clean.pdf](#) (in English only).

⁵ NERC Project 2023-03, retrieved on March 17th, 2026: [2023-03 Internal Network Security Monitoring \(INSM\)](#) (in English only).

1.5. Proposed effective dates

The implementation plan of the *reliability standard* of CIP-015-1 proposes that the standard comes into effect on the first day of the first civil quarter occurring 36 months after the regulatory body's approval of the standard. In the United States, the CIP-015-1 will come into effect on October 1st, 2028⁶. From that date, a phased compliance schedule applies. The entity responsible for the control and backup centers identified in accordance with requirement R1, paragraphs 1.1 and 1.2 of CIP-002-5.1a must comply within this 36-month period, whereas any responsible entity that owns *BES*-electronic systems with routable external connectivity, except for the previously mentioned control and backup centers, has an additional period of up to 24 calendar months following the effective date of the standard.

This gradual approach acknowledges the technical and organizational complexity associated with the implementation of internal monitoring solutions, including the structured collection and analysis of network data, the adjustment of existing architectures, and staff training.

The Reliability Coordinator considers that the criteria established by the Régie, requiring enforcement on the first day of a calendar quarter⁷ and a minimum period of sixty (60) days⁸ between the date of adoption and the entry into force of a standard, are met within the framework of the NERC implementation plan.

Given the importance of having uniform practices with mandatory standards harmonized with the United States, the Coordinator proposes an effective date on the first day of the first civil quarter occurring thirty-six (36) months after the adoption of the reliability standard by the Régie. For certain *BES*-electronic systems with routable external connectivity under standard CIP-015-1, the Reliability Coordinator proposes the same implementation deadlines granted to entities in the United-States.

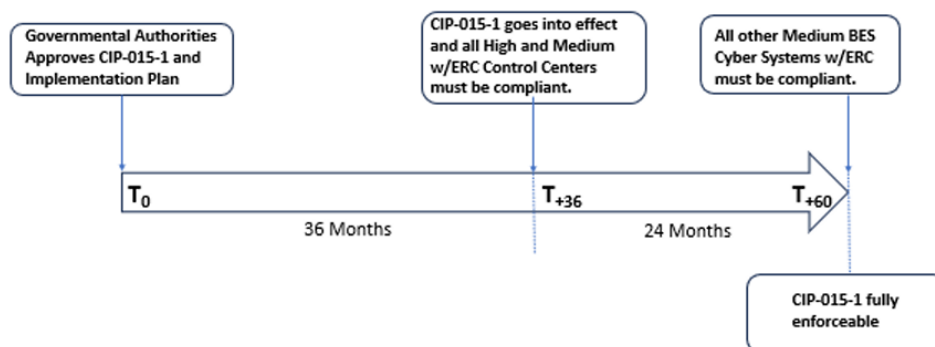


Figure 1. Implementation timeline by the NERC for the reliability standard CIP-015-1.⁹

1.6. Standard to retire

No standard to retire.

⁶ United States Mandatory Standards Subject to Enforcement, retrieved on March 17th, 2026:

<https://www.nerc.com/pa/Stand/Pages/USRelStand.aspx> (in English only).

⁷ In Decision [D-2015-168](#), the Régie set the effective date of standards as the first day of the calendar quarters following the date of adoption.

⁸ In Decision [D-2016-011](#), the Régie set a minimum of 60 days between the adoption of standards and their effective date.

⁹ Implementation timeline by the NERC Implementation plan for project 2023-03 (p.3/3), retrieved on March 17th, 2026: <https://www.nerc.com/globalassets/standards/projects/2023-03/2023-03-implementation-plan-fb-clean.pdf> (in English only).

1.7. Modifications to the glossary

No changes to the Glossary.

2. ASSESSMENT OF RELEVANCE

The *reliability standard* CIP-015-1 aims to establish policies requiring applicable entities to implement an internal network security monitoring plan for high-impact *BES* Cyber Systems, whether they have external routable connectivity or not, as well as for moderate-impact *BES* Cyber Systems with external routable connectivity, aiming to detect unauthorized activities within the cyber perimeter. The standard notably requires the detection and assessment of anomalies, the retention of monitoring data, and the protection of the integrity of that data, thereby facilitating potential investigations and incident management. To achieve this objective, CIP-015-1 contains three primary requirements. Requirement R1 obligates responsible entities to implement documented processes to monitor, detect, and evaluate any anomalous or unauthorized activity within the Electronic Security Perimeter (*ESP*) of *BES* Cyber Systems. The second requirement R2 specifies the retention of monitoring data for a minimum defined period to support investigations and compliance verification. Finally, the third requirement R3 requires that monitoring data be protected against unauthorized modification or deletion. In order to comply with these requirements, responsible entities may need to acquire sensors to facilitate network data collection on applicable networks and implement modifications to their networks to better align them with standard CIP-015-1.

The NERC is of the view that the standard proposed for adoption is reasonable, is not unduly discriminatory or preferential, and is in the public interest¹⁰. The FERC concluded in Order 907¹¹ that the NERC's rationale is supported by the fact that the new *reliability standard* enhances the Cyber security of the *BES* by requiring applicable entities to implement internal network security monitoring mechanisms to ensure the detection of anomalous network activities indicative of an ongoing attack.

Additionally, the New Brunswick Energy and Utilities Board approved standard CIP-015-1-NB-0 on October 31st, 2025, under proceeding n° ER-004-2025¹², with an effective date scheduled for January 1st, 2029. In Ontario, the project was approved by the Ontario Energy Board on May 9th, 2024¹³.

The relevance of the *reliability standard* CIP-015-1 is based on improving intrusion detection methods within operational networks themselves. Transmission infrastructures rely on numerous cyber systems, including SCADA systems, control centers, digital protection relays, and telecommunications equipment. Although these systems are generally protected by perimeter controls imposed by existing CIP standards, a successful attack could allow a malicious entity to move laterally within the internal network. For the entities concerned, the application of this standard could therefore result in the implementation or strengthening of industrial network traffic monitoring technologies, behavioral analytics, and data collection from environments containing critical cyber systems. These measures would improve visibility over internal network communications and enable faster detection of cybersecurity incidents, thereby reducing risks to the *Main Transmission System (MTS)*.

¹⁰ Notice of filing of the NERC for CIP-015-1 (p.1), retrieved on March 17th, 2026: https://www.nerc.com/globalassets/who-we-are/membership/legal--regulatory/ca/filings--orders/qb-notice-of-filing-of-cip-015-in-sm_packaged.pdf (in English only).

¹¹ FERC Order 907, retrieved on March 17th, 2026: https://elibrary.ferc.gov/eLibrary/filelist?accession_num=20250626-3039 (in English only).

¹² New Brunswick Project n° 555, retrieved on March 17th, 2026: <https://filemaker.nbeub.ca/fmi/webd/NBEUB%20Toolkit13>

¹³ Ontario Energy Board Review Process, retrieved on March 17th, 2026: <https://www.ieso.ca/en/Sector-Participants/System-Reliability/OEB-Review-Process> (in English only).

Considering the elements mentioned above regarding CIP-015-1, and knowing that this standard was developed by recognized organizations in North America, including in Québec and in neighboring jurisdictions, in accordance with the agreement concluded in 2009 between the Régie, the NERC and the NPCC with the authorization of the Government of Québec¹⁴, the Reliability Coordinator is of the opinion that *reliability standard* CIP-015-1 contributes to the reliability of the Québec system and to harmonization with *neighboring networks*.

3. PRELIMINARY IMPACT ASSESSMENT

This section presents the preliminary assessment of the impact on all entities in Québec according to the Reliability Coordinator.

The preliminary impact resulting from the implementation of the *reliability standard* CIP-015-1 in Quebec can be considered moderate, given that the standard requires applicable entities to deploy internal network security monitoring technologies capable of detecting anomalous activity within the *Electronic Security Perimeter* (ESP) of high-impact BES Cyber Systems with or without External Routable Connectivity, and medium-impact systems that possess External Routable Connectivity. This will require monitoring tools, data collection, and internal traffic analysis processes, which could require interruptions to operational facilities and/or the implementation of capabilities to ingest large volumes of network information and perform the necessary analysis.

Since several other CIP cybersecurity measures are already in place and are responsible for numerous fundamental Cyber security controls, the introduction of internal network monitoring within trust zones requires additional modifications to the architecture, including additional sensors, data retention systems, and anomaly detection processes. These deployments may require technical integration across operational networks. Consequently, the implementation risk is considered moderate, as new technologies must be integrated into existing control systems without disrupting network operations.

The impact of maintaining the new infrastructure can be considered low since, once the monitoring infrastructure has been deployed, responsible entities are only required to maintain the associated sensors, update detection rules, and ensure the retention of monitoring data and its protection against unauthorized modification. These additional maintenance requirements are partially mitigated by the presence of Cyber security governance mechanisms already established as part of the critical infrastructure protection program. Entities are already required to maintain cybersecurity management processes, personnel training programs, and system documentation in accordance with standards such as standards CIP-003 and CIP-004.

Finally, the impact associated with regulatory follow-up and oversight related to the coming into force of CIP-015-1 is low. In this context, the Reliability Coordinator in Quebec conducts consultations with relevant entities and submits proposed standards to the Régie for adoption prior to their enforcement. Since this regulatory integration process, the introduction of CIP-015-1, as well as its subsequent version CIP-015-2, should remain essentially procedural.

¹⁴ Agreement entered into pursuant to Decree No. 443-2009 issued on April 8th, 2009. http://www.regie-energie.qc.ca/audiences/normes_fiab_tranp_elec/Entente_Regie_NERC_NPCC_5mai09.pdf

The table below shows preliminary assessments of the impact on all Québec entities.

Standard	Impact		
	Implementation	Enforcement	Monitoring
CIP-015-1	Moderate	Low	Low

Legend:

- Low:** Normal industry practice or standard that only requires minor adjustments to existing processes or practices.
- Moderate:** Change that requires the mobilization of some physical, human or financial resources to implement the proposed standard, enforce it or monitor compliance.
- High:** Change that requires provision and mobilization of significant physical, human or financial resources to plan and implement the proposed standard, enforce it or monitor compliance.

4. FINAL IMPACT ASSESSMENT

This section will be completed upon receipt of the impact assessment forms and at the conclusion of the consultation process prior to filing of the standards with the Régie.